# Planning the Installation



# Topology Options

This section provides an overview of the system topology and describes the relationship between the types of nodes in the topology.

### Clusters

Clusters provide a mechanism for distributing call processing, presence status, and database replication among multiple servers. They provide transparent sharing of resources and features, and enable system scalability.

A cluster comprises a set of Unified Communications Manager nodes and  IM and Presence nodes that run compatible software versions.

### Publisher Nodes and Subscriber Nodes

Within a cluster, there is a database publisher for each type of node that you install.

When you install Unified Communications Manager, the installation wizard prompts you to specify whether the node you are installing is the first node in the cluster. The first Unified Communications Manager node that you install becomes the publisher node, because it publishes the voice and video database to the other Unified Communications Manager nodes in the cluster. All subsequent nodes in the cluster are called subscriber nodes. Each subscriber node must be associated with the publisher node. You must set up all subscriber nodes in the system topology on the publisher node before you install the software on the subscriber nodes.

When you install IM and Presence nodes, the first node that you install functions as the server for the IM and Presence database. Because this node publishes the database for all of the IM and Presence nodes in the cluster, it is referred to as the IM and Presence database publisher; however, you must install this and all other IM and Presence nodes as subscribers of the Unified Communications Manager publisher node. As with other subscriber nodes, you must add these in the system topology before you install the software.

### Topology Options

When installing your cluster, you must decide on the topology that you want to deploy. For example:

- The number of cluster nodes required.
- Whether you will install all cluster nodes in a single location, or if you will install your nodes in separate geographic sites connected via a WAN in order to provide geographic redundancy. For more information on scalability, see Megacluster.

# Cluster Topology for IM and Presence

If you are deploying the IM and Presence Service, you must decide before you begin the installation whether you want a Standard Deployment (IM and Presence Service on Unified Communications Manager) or an IM and Presence Centralized Cluster Deployment.

| IM and Presence Deployment | Description |
|---|---|
| Standard Deployment (de-centralized/distributed) ) | The IM and Presence Service cluster nodes are installed on the physical servers as the Unified Communications Manager telephony cluster. The IM and Presence cluster shares a platform and many of the same services as the telephony cluster. This option requires a 1x1 mapping of Unified CM telephony clusters to IM and Presence clusters.<br><br>Basic installations order followed is same as mentioned in the Attended Install method. For more information, see the "Installation Methods".<br><br>For touchless installations, you can install all Unified Communications Manager and IM and Presence Service cluster nodes concurrently in a single process. |

| IM and Presence Deployment | Description |
|---|---|
| IM and Presence Centralized Cluster Deployment | The IM and Presence Service central cluster is installed separately from your telephony cluster and may be located on different hardware servers. This deployment removes the 1x1 mapping requirement between telephony clusters and IM and Presence clusters. This allows you to scale your telephony deployment and IM and Presence deployment separately.<br><br>For basic installations:<br><br>1. Install a local Unified Communications Manager publisher node in the central cluster. This node is not a part of your telephony deployment. The node handles functions like database and user provisioning for the central cluster.<br>2. Install the IM and Presence Service database publisher node.<br>3. Install any IM and Presence subscriber nodes.<br><br>For touchless installations, you can install your local Unified Communications Manager publisher node and your IM and Presence Service central cluster in a single process. However, your telephony cluster must be installed separately.<br><br>For more information, see the "Configure Centralized Deployment" chapter at Configuration and Administration of the IM and Presence Service Guide. |

# Installation Methods

This guide covers the installation methods for Unified Communications Manager and IM and Presence Service.

These installation methods can be used for any of the following scenarios:

- Fresh Install (first-time setup of a brand-new node or cluster, no existing deployment, and no existing customer data).
- Expand a cluster (add a new subscriber node to an existing cluster).
- Direct Migration from an older version. For more information, see the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.

| Installation Method | Description |
| --- | --- |
| Attended Install | A baseline-typical installation of one node of either Unified Communications Manager or IM and Presence Service, using the native Install Wizard graphical user interface (GUI). Unified Communications Manager only includes an option **Apply a Patch During an Upgrade** (for example, to apply a Service Update to the base release you are installing).<br><br>To install a cluster using this method, follow the Attended Installation steps in this sequence:<br><br>• Unified Communications Manager publisher node<br>• Unified Communications Manager subscriber nodes<br>• IM and Presence Service publisher node<br>• IM and Presence Service subscriber nodes<br><br>You can use this method with any of the following software media options:<br><br>• Physical install DVD.<br>• Bootable installer image for base release in ISO format (obtained from either Cisco Commerce Workspace, My Cisco Entitlements, or a Cisco Business Edition appliance factory preload).<br>• Deployed OVA containing preinstalled application. This OVA format file contains fully installed, ready-to-run application, obtained from a Cisco Business Edition appliance factory preload.<br>• Partial skip-installed OVA. This OVA format file contains partially installed application up to the "skip" Install Wizard point where the application is ready to accept an Answer File and complete installation. OVA format file is obtained either from My Cisco Entitlements or from a Cisco Business Edition appliance factory preload.<br><br>**Note** Use this method when manual installation without automation is acceptable, such as labs or small deployments. |

| Installation Method | Description |
| --- | --- |
| Touchless Install of a Single Node or a Cluster | A partially automated installation of one node or installation of clusterwide install of multiple nodes of Unified Communications Manager and IM and Presence Server.<br><br>Use this method to get basic automation for one node, where you can fill out all the information initially, start the Install Wizard with that information, and complete the rest of the installation automatically using the Answer File.<br><br>For clusterwide installations, use this method to generate pre-created Answer Files, that occurs in one seamless process with minimal intervention.<br><br>To install a single node or a cluster using this method, follow the Touchless Install of Cluster steps:<br><br>**1.** Create an Answer File for each node or node in the cluster using the Unified Communications Answer File Generator.<br><br>**2.** Place all those Answer Files in well-known locations. See Generate Answer Files for Touchless Install.<br><br>**3.** Power on the node or all the cluster nodes simultaneously.<br><br>In this method, no interaction with the native Install Wizard is required. The nodes will communicate with each other and each node will read its Answer File for instructions.<br><br>You can use this method with any of the software media options available for Attended Install. Use this method to:<br><br>• Get more automation—Unattended Install of the entire cluster + zero interaction with the native Install Wizard.<br><br>• Faster installation—Cluster nodes undergo installation in parallel. This is especially useful if you have a large cluster with many nodes to install. |

| Installation Method | Description |
|---|---|
| Cisco Prime Collaboration Deployment (PCD) | Fresh install, add nodes to, or direct migrate a cluster of Unified Communications Manager and IM and Presence Server using Cisco Prime Collaboration Deployment. See the *Cisco Prime Collaboration Deployment Administration Guide* for the following:<br>• Fresh Install Task (where PCD performs similar operation as Touchless Install of a Single Node or Cluster).<br>• Edit/Expand Task (where PCD performs similar operation as Touchless Install to add a single node).<br>• Migration Task (where PCD is performing direct migration of an entire cluster).<br><br>Use this method when:<br>• You require assistance with multiple nodes of one cluster and/or multiple clusters, and a separate management application is acceptable.<br>• (PCD Migration Task only) you are "repaving" an existing installation where you are dealing with one or more of the following:<br>  • Two or more of these factors as part of the same migration—site moves, hardware changes, VMware upgrades, application version upgrades, application readdresses, and in scenarios where more flexibility is expected than what direct upgrades can provide.<br>  • You need to rebuild, restore or recover a cluster, or you need to revert configuration changes. Here, you are looking for a more flexible approach than what Unified Communications Manager Disaster Recovery Solution can provide.<br>  • It is acceptable to leverage application readdress and temporary extra hardware footprint to reduce migration downtime or duration. |

| Installation Method | Description |
|---|---|
| VMware OVF Tool | Allows you to perform fully automated installation or direct migration of either a single node or an entire cluster, using the VMware OVF Tool.<br><br>To install or direct migrate a cluster, follow the procedures at Automated Installation using vApp properties and VMware OVF Tool:<br><br>• Use the VMware OVF Tool to create a skip-install OVA for each cluster node (with OVA parameters filled in, instead of using Answer File Generator).<br><br>• Deploy all cluster nodes skip-installed OVAs simultaneously.<br><br>• Installation continues like Touchless Install of a Single Node or Cluster or Fresh Install with Data Import.<br><br>It is best to use this method with skip-install OVAs, as that provides the shortest duration and highest level of automation.<br><br>Use this method when you require a programmatic install or direct migration method on top of any of the factors that drive consideration of Touchless Install of Cluster or Fresh Install with Data Import. |

| Installation Method | Description |
|---|---|
| Fresh Install with Data Import | Perform direct migration of either a single node or an entire cluster, using similar mechanisms as Prime Collaboration Deployment Migration task but native to Unified Communications Manager and IM and Presence.<br><br>To directly migrate a cluster, follow the Fresh Install with Data Import tasks:<br><br>• On each cluster node, export your old version's data.<br><br>• For each cluster node, provision a new virtual machine for your new version and follow either Attended Install or Touchless Install for a single node or the cluster node(s) of interest. Using the Data Import options available in Install Wizard and/or the Unified Communications Answer File Generator.<br><br>You can use this method with any of the software media options available for Attended Install.<br><br>Use this method for "native" direct migrations that don't require a separate management application like Prime Collaboration Deployment. You can have more granular control over individual nodes migration timing and sequencing. You may also use this method to avoid use of application readdress and temporary extra hardware footprint for direct migration. |
| Node Installs | If you want to add a node to an existing Unified Communications Manager or IM and Presence Service cluster for attended or touchless installation, complete the tasks in:<br><br>Add a New Node to an Existing Cluster |

# Requirements and Limitations

The following sections provide information about the requirements that your system must meet, and limitations that apply when you install or upgrade Unified Communications Manager or IM and Presence Service.

**Note**

- By default, your system is in non-FIPS mode, you must enable it, if desired.
- Ensure that the security password length is minimum 14 characters before you enable FIPS, Common Criteria, or Enhanced Security mode on the cluster. Update the password even if the prior version was FIPS enabled.

**Note** Unified Communications Manager 14 requires minimum ESXi version of 6.7 U2 with minimum VM Hardware version of 13. For more information on latest Unified Communications Manager ESXi version support, see http://www.cisco.com/go/virtualized-collaboration.

# Subnet Limitations

Do not install Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices. For more information, see Cisco Collaboration System 12.x Solution Reference Network Designs (SRND).

# Cluster Size

The number of Unified Communications Manager subscriber nodes in a cluster cannot exceed 4 subscriber nodes and 4 standby nodes, for a total of 8 subscribers. The total number of servers in a cluster, including the Unified Communications Manager publisher node, TFTP server, and media servers, cannot exceed 21.

The maximum number of IM and Presence Service nodes in a cluster is 6.

For more information, see *"Cisco Collaboration Solutions Design Guidance"* at http://www.cisco.com/go/ucsrnd.

# IP Address Requirements

A complete collaboration solution relies on DNS in order to function correctly for a number of services and thus requires a highly available DNS structure in place. If you have a basic IP telephony deployment and do not want to use DNS, you can configure Unified Communications Manager and IM and Presence Service to use IP addresses rather than hostnames to communicate with gateways and endpoint devices.

You must configure the server to use static IP addressing to ensure that the server obtains a fixed IP address. Using a static IP address also ensures that Cisco Unified IP Phones can register with the application when you plug the phones into the network.

# DNS requirements

Note the following requirements:

- Mixed-mode DNS deployments not supported—Cisco does not support mixed-mode deployments. Both Unified Communications Manager and IM and Presence Service must either use or not use DNS.
- If your deployment uses DNS—Unified Communications Manager and IM and Presence Service should use the same DNS server. If you use different DNS servers between IM and Presence Service and Unified Communications Manager, it is likely to cause abnormal system behavior.
- If your deployment does not use DNS, you will need to edit the following Host Name/IP Address fields:
  - Server—In the Cisco Unified CM Administration **Server Configuration** window, set IP addresses for your cluster nodes.

- IM and Presence UC Service—In the Cisco Unified CM Administration **UC Service Configuration** window, create an IM and Presence UC service that points to the IP address of the IM and Presence database publisher node.
- CCMCIP Profiles—In the Cisco Unified CM IM and Presence Administration **CCMCIP Profile Configuration** window, point any CCMCIP profiles to the IP address of the host.

- Multinode considerations—If you are using the multinode feature in IM and Presence Service, see the section regarding multinode deployments in the Configuration and Administration of the IM and Presence Service Guide for DNS configuration options.

# Firewall Requirements

Ensure that you configure your firewall so that connections to port 22 are open, and aren't throttled. During the installation of Unified Communications Manager and IM and Presence subscriber nodes, multiple connections to the Unified Communications Manager publisher node are opened in quick succession. Throttling these connections could lead to a failed installation. For general security considerations, see the Security Guide for Cisco Unified Communications Manager.

**Note** We recommend that you disable the "Intruder/Intrusion Detection" and/or "Brut Force Attack" features during upgrade and installs because these Firewall features are known to cause upgrades and installations to fail.

For more information on the port usage, see the chapter 'Cisco Unified Communications Manager TCP and UDP Port Usage' in the System Configuration Guide for Cisco Unified Communications Manager.

# Platform Requirements

This section provides information about the platform requirements that you must meet before you can deploy Unified Communications Manager and the IM and Presence Service on virtual machines.

In this release, you cannot install or run Unified Communications Manager and the IM and Presence Service directly on server hardware; you must run these applications on virtual machines.

Before you can install or upgrade the software on a virtual machine, you must:

- configure the platform
- install and configure ESXi virtualization software

**Note** Unified Communications Manager 14 requires minimum ESXi version of 6.7 U2 with minimum VM Hardware version of 13. For latest Unified Communications Manager ESXi version support, see https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html.

- deploy a virtual machine from the correct Cisco provided OVA file for the release. Depending on the installation method used, additional steps are required.

# Supported Versions

Unified Communications Manager and the IM and Presence Service nodes in the same cluster must be running the supported builds as mentioned in the Release Notes for Cisco Unified Communications Manager and the IM and Presence Service.

### Version Mismatches

This release offers two main deployment options for this release of Unified Communications Manager and the IM and Presence Service:

- Standard Deployments of IM and Presence Service—Both Unified Communications Manager and the IM and Presence Service must be running the supported versions for your deployment. A version mismatch is not supported.
- Centralized Deployments of IM and Presence Service—If you have the Centralized Deployment option configured on the IM and Presence Service, then within the IM and Presence Service central cluster, both the Unified Communications Manager instance and the IM and Presence Service must be running the same version. However, the telephony cluster that the central cluster connects to does not have to be running the same version.

**Note** The Centralized IM and Presence Service cluster requires a Unified CM publisher node, for a total of 7 servers in the cluster: 3 IM and Presence sub-cluster pairs (6 servers) + the Unified CM publisher node

# Software Restrictions

You cannot install or use third-party or Windows-based software applications. The system can upload and process only software that Cisco Systems provides and digitally signs. For more information, see the 'Operating System and Security Hardening' chapter in the Security Guide for Cisco Unified Communications Manager.

You must perform all software installations and upgrades using Cisco Unified Communications Operating System Administration.

For information about software compatibility for Unified Communications Manager and IM and Presence Service, see the Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service.

# Username and Password Requirements

During the installation, you must specify the following user names and passwords:

- Administrator Account user name and password
- Application User name and password
- Security password

### Administrator Account

You use the Administrator Account user name and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration
- Disaster Recovery System
- Command Line Interface

To specify the Administrator Account user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator Account password or add a new Administrator account by using the command line interface. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

### Application User

When you install Unified Communications Manager, you must enter an Application User name and password. You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Real-Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application User name and password, follow these guidelines:

- Application User username—The Application User username must start with an alphabetic character and can contain alphanumeric characters, hyphens, and underscores.
- Application User password—The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

**Caution** Do not use the system application name as the Application User name. Using a system application name causes the installation to fail with an unrecoverable error during the installation of the database.

System application names are:

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

You can change the Application User name and password by using the command line interface. For more information, see the Command Line Interface Reference Guide for Cisco Unified Communications Solutions.

### Security Password

During the installation, you must specify a security password. Unified Communications Manager systems use this password to authorize communications between nodes in the cluster, including IM and Presence Service nodes. This password must be identical on all nodes in the cluster.

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

## Password Recommendations

The installation wizard ensures that you enter a strong password. To create a strong password, follow these recommendations:

- Password must be at least 6 characters long and can contain alphanumeric characters, hyphens, and underscore.

**Note** If you plan to enable FIPS, Common Criteria, or Enhanced Security mode on any cluster, you must ensure that the security password is at least 14 characters long.

- Should not have the non-printable ASCII characters.
- Contains at least one alphanumeric character.
- Mix uppercase and lowercase letters.
- Mix letters and numbers.

- Include special symbols.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use only alphanumeric characters.
- Do not use any non-alphanumeric characters.
- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert-recognizable words.
- Do not use word or number patterns, such as aaabbb, abc123, qwerty, zyxwvuts, and 123321.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children, or pets.

# Installation Time Requirements

### Time Requirements for Unified Communications Manager

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes, depending on your server type.

### Time Requirements for IM and Presence Nodes

The entire IM and Presence Service installation process, excluding pre- and post-installation tasks, takes approximately 45 to 90 minutes per server, depending on your server type.

# Licensing Requirements

The following sections provide information about the licensing requirements for Unified Communications Manager and the IM and Presence Service.

**Note** As of Unified Communications Manager Release 12.0(1), Smart Licensing replaces Prime License Manager. Smart Licensing requires you to have a Smart Account created and configured before you upgrade or migrate the Unified Communications Manager server.

Several deployment options through which Unified Communications Manager can connect to Cisco Smart Software Manager or Cisco Smart Software Manager satellite are:

- Direct—Unified Communications Manager sends usage information directly over the internet. No additional components are needed.
- Cisco Smart Software Manager satellite—Unified Communications Manager sends usage information to an on-premise Smart Software Manager. Periodically, an exchange of information is performed to

keep the databases in synchronization. For more information on installation or configuration of the Smart Software Manager satellite, go to this URL: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

**Note** Cisco Smart Software Manager satellite is an on-premises collector similar to standalone Prime License Manager.

- Proxy Server—Unified Communications Manager sends usage information over the internet through a proxy server.

# Unified Communications Manager License Requirements

Cisco Smart Software Licensing is a new way of thinking about licensing. It adds flexibility to your licensing and simplifies it across the enterprise. It also delivers visibility into your license ownership and consumption.

Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for product activation keys (PAK). It pools license entitlements in a single account and allows you to move licenses freely through the network, wherever you need them. It is enabled across Cisco products and managed by a direct cloud-based or mediated deployment model.

The Cisco Smart Software Licensing service registers the product instance, reports license usage, and obtains the necessary authorization from Cisco Smart Software Manager or Cisco Smart Software Manager satellite.

Cisco Smart Software Manager replaces Prime License Manager in Unified Communications Manager Release 12.0(1) and later versions. Cisco Prime License Manager is no longer used as of Release 12.0(1) and no longer appears in the Installed Applications pre-login screen.

If you have enabled the mixed-mode before upgrade and have not registered to Cisco Smart Software Manager or Cisco Smart Software Manager satellite then,

- You see the warning message in the Cisco Unified CM Administration page and Cisco Unified OS Administration page as stated below:

**Caution** The system is currently running Mixed mode. To continue running Mixed mode, please ensure Smart Licensing registration is completed using the Registration Token received from the Smart/Virtual Account that has Allow export-controlled functionality checked.

- An alert named *SmartLicenseExportControlNotAllowed* is sent, when the Unified Communications Manager is not registered with the Registration Token.

For details on how to configure Cisco Smart Software Licensing, see the "Smart Software Licensing" chapter, located within the "Configure Initial Parameters for the System" at System Configuration Guide for Cisco Unified Communications Manager.

For more details on Cisco Smart Software Manager satellite, including the *Smart Software Manager satellite Installation Guide*, see http://www.cisco.com/go/smartsatellite.

### Migration of PLM Licenses to Smart Entitlement

If you are eligible to upgrade to the Smart Licensing version of the product, then you are able to initiate the migration through the License Registration Portal or Cisco Smart Software Manager. You can self-initiate this process by downloading and installing the Smart Licensing version of the software and registering the device to a Smart Account using a Registration Token. The migration of any entitlements tracked by Cisco automatically migrates to the Customers Smart Account. You will also be able to initiate the migration of unused classic PAKs to Smart Accounts for future consumption by products in Smart Mode. This process is available through the License Registration Portal or Cisco Smart Software Manager.

**Unified Communications Manager 9.0x and later version of 12.0(1)**

- If you are holding an active Cisco Software Support Service (SWSS) contract, then you can convert the classic licenses to smart entitlements through the Cisco Smart Software Manager at https://software.cisco.com/#SmartLicensing-LicenseConversion.
- Two types of Migration are supported:
  - PAK based—Supported for already fulfilled, partially fulfilled and unfilled PAKs
  - Device based
- Partial Conversion supports mixed environment of older and Unified Communications Manager 12.0(1) clusters.

### Upgrade to Smart Entitlement

**Unified Communications Manager Pre 9.0x (Device based) to 12.0(1)**

You may contact Cisco Global Licensing Operations (GLO) for helping with migrating Device-based licenses to Smart Entitlement.

Customer may establish equivalent user-based licensing required by running License Count Utility (LCU). For more details, see http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/upgrade/uct/CUCM_BK_UCT_Admin_Guide/CUCM_BK_UCT_Admin_Guide_chapter_01.html.

From the LCU report, Customer may order respective quantity of Upgrade Licenses through Cisco Commerce Workspace. Beyond this, they would have to buy additional new licenses. For more details, see the Ordering Guide at http://www.cisco.com/c/en/us/partners/tools/collaboration-ordering-guides.html.

# IM and Presence Service License Requirements

The IM and Presence Service does not require a server license or software version license. However, you must assign users and enable the IM and Presence Service for each assigned user.

**Note** With the Jabber for Everyone offer, no end user licenses are required to enable IM and Presence Service functionality. For more information, see Jabber for Everyone Quick Start Guide.

You can assign IM and Presence Service on a per user basis, regardless of the number of clients you associate with each user. When you assign IM and Presence Service to a user, this enables the user to send and receive IMs and availability updates. If users are not enabled for IM and Presence Service, they will not be able to log in to the IM and Presence Service server to view the availability of other users, send or receive IMs, and other users will not see their availability status.

You can enable a user for IM and Presence Service using any of the following options:

- The **End User Configuration** window in Unified Communications Manager. For more information, see the Administration Guide for Cisco Unified Communications Manager.
- The Bulk Administration Tool (BAT)
- Assign IM and Presence Service to a feature group template which you can reference from the **Quick User/Phone Add** window in Unified Communications Manager.

For more information, see the System Configuration Guide for Cisco Unified Communications Manager.

IM and Presence Service capabilities are included within both User Connect Licensing (UCL) and Cisco Unified Workspace Licensing (CUWL). IM and Presence Service capabilities can also be acquired for users that are not Unified Communications Manager IP Telephony users through the Jabber for Everyone Offer. For more information, see Jabber for Everyone Quick Start Guide.

# Required Installation Information

When you install either Unified Communications Manager or the IM and Presence Service on a server, the installation process requires you to provide specific information. You can provide this information manually during the installation process or you can provide it using an answer file. For each server that you install in a cluster, you must gather this information before you begin the installation process.

The following table lists the information that you must gather before you begin the installation.

**Note** Because some of the fields are optional, they may not apply to your configuration. For example, if you decide not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.

You cannot change some of the fields after the installation without reinstalling the software, so be sure to enter the values that you want. The last column in the table shows whether you can change a parameter after installation, and if you can, it provides the appropriate menu path or Command Line Interface (CLI) command.

We recommend that you make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.

***Table 1: Required Installation Information***

| Configuration Data | Description | Editable after Installation |
|---|---|---|
| **Administrator Credentials** | | |
| Administrator Login | Specifies the name that you want to assign to the Administrator account. | No<br>After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID. |
| Administrator Password | Specifies the password for the Administrator account. | Yes<br>CLI: `set password user admin` |

| Configuration Data | Description | Editable after Installation |
|---|---|---|
| **Application User Credentials** | | |
| Application User Username | Specifies the user ID for applications installed on the system. | Yes<br>CLI: **utils reset_application_ui_administrator_name** |
| Application User Password | Specifies the password for applications on the system. | Yes<br>CLI: **utils reset_application_ui_administrator_password** |
| **Security Password** | | |
| Security password for Unified Communications Manager | Servers in the cluster use the security password to communicate with one another. Set this password on the Unified Communications Manager publisher node, and enter it when you install each additional node in the cluster, including IM and Presence nodes. | Yes. You can change the security password on all nodes in the cluster using the following command:<br>CLI: **set password user security** |
| **Certificate Information** | | |
| Organization | Used to create the Certificate Signing Request. | Yes<br>CLI: **set web-security [orgunit] [orgname] [locality] [state] [country]** |
| Unit | Used to create the Certificate Signing Request. | Yes<br>CLI: **set web-security [orgunit] [orgname] [locality] [state] [country]** |
| Location | Used to create the Certificate Signing Request. | Yes<br>CLI: **set web-security [orgunit] [orgname] [locality] [state] [country]** |
| State | Used to create the Certificate Signing Request. | Yes<br>CLI: **set web-security [orgunit] [orgname] [locality] [state] [country]** |

| Configuration Data | Description | Editable after Installation |
|---|---|---|
| Country | Used to create the Certificate Signing Request. | Yes<br>CLI: **`set web-security [orgunit] [orgname] [locality] [state]`** |
| **(Optional) SMTP** | | |
| SMTP Location | Specifies the name of the SMTP host that is used for outbound email.<br>You must fill in this field if you plan to use electronic notification. If not, you can leave it blank. | Yes<br>• In Cisco Unified Communications Operating System Administration: select **Settings** > **SMTP** and enter the IP address or Hostname in the SMTP Host Field.<br>• CLI: **`set smtp [host]`** |
| **NIC Interface Settings** | | |
| NIC Speed | If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) speed, you must select the NIC speed (either 10 megabit or 100 megabit). | Yes<br>CLI: **`set network nic eth0 {auto \| {en\| dis}} {speed\| {10\| 100}} {duplex half\| {half\| full}}`**<br>**Note** 1000BASE-T can only be enabled via auto-negotiation.<br>**Note** Virtual machines do not support this command. |
| NIC Duplex | If you do not enable automatic negotiation of the ethernet Network Interface Card (NIC) duplex setting, you must select the NIC duplex setting (either Full or Half). | Yes<br>CLI: **`set network nic eth0 {auto \| {en\| dis}} {speed\| {10\| 100}} {duplex half\| {half\| full}}`**<br>**Note** 1000BASE-T can only be enabled via auto-negotiation.<br>**Note** Virtual machines do not support this command. |

| Configuration Data | Description | Editable after Installation |
|---|---|---|
| MTU Size<br>**Note** The MTU setting must be the same on all nodes in a cluster. | The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host transmits on the network.<br>The value must not exceed the lowest MTU size that is configured on any link in your network.<br>Default: 1500 bytes | Yes<br>CLI: **`set network mtu [size]`** |
| **Network Information** | | |
| DHCP<br>(Dynamic Host Configuration Protocol) | Select **Yes** if you want to use DHCP to automatically configure the network settings on your server.<br>If you select **No**, you must enter a hostname, IP Address, IP Mask, Gateway, and DNS configuration. | Yes.<br>• In Cisco Unified Operating System Administration: select **Settings** > **IP** > **Ethernet**.<br>• CLI: **`set network dhcp eth0 [enable]`**<br>CLI: **`set network dhcp eth0 disable [node_ip] [net_mask] [gateway_ip]`** |
| Hostname | If DHCP is set to No, you must enter a hostname for this machine. | Yes; for Unified Communications Manager nodes, choose one of the following:<br>• In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet**.<br>• CLI: **`set network hostname`**<br>You will be prompted to enter the parameters.<br>To change the hostname on Unified Communications Manager or IM and Presence server, see the 'IP Address, Hostname, and Domain Name Changes' section in the Administration Guide for Cisco Unified Communications Manager. |

| Configuration Data | Description | Editable after Installation |
|---|---|---|
| IP Address | If DHCP is set to No, you must enter the IP address of this machine. | Yes; for Unified Communications Manager nodes, choose one of the following:<br>• In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet**.<br>• CLI: **`set network IP eth0 [ip-address] [ip-mask]`**<br>To change the IP address on Unified Communications Manager or IM and Presence server, see see the 'IP Address, Hostname, and Domain Name Changes' section in the Administration Guide for Cisco Unified Communications Manager. |
| IP Mask | If DHCP is set to No, you must enter the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address.<br>The subnet mask must use the following format: 255.255.255.0 | Yes<br>• In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet**.<br>• CLI: **`set network IP eth0 [ip-address] [ip-mask]`** |
| Gateway Address | If DHCP is set to No, you must enter the gateway address. | Yes<br>• In Cisco Unified Communications Operating System Administration, select **Settings** > **IP** > **Ethernet**.<br>• CLI: **`set network gateway [addr]`** |
| **(Optional) DNS** | | |
| DNS Primary | If you have a Domain Name Server (DNS), IM and Presence contacts this DNS server first when attempting to resolve hostnames. | Yes<br>CLI: **`set network dns primary [address]`** |
| DNS Secondary | When a primary DNS server fails, IM and Presence will attempt to connect to the secondary DNS server. | Yes<br>CLI: **`set network dns secondary [address]`** |

| Configuration Data | Description | Editable after Installation |
|---|---|---|
| Domain | Represents the name of the domain in which this machine is located | Yes<br>CLI: `set network domain [name]` |
| **Timezone** | | |
| Time Zone | Reflects the local time zone and offset from Greenwich Mean Time (GMT). Select the time zone that most closely matches the location of your machine. | Yes<br>CLI: `set timezone [zone` |
| **Network Time Protocol** | | |
| NTP Server IP Address | During installation of the IM and Presence publisher node, you must specify the IP address of an external Network Time Protocol (NTP) server. We recommend that you use the Unified Communications Manager publisher node as the NTP server. | Yes<br>In Cisco Unified Communications Operating System Administration, select **Settings** > **NTP Servers**. |

# Export Restricted and Export Unrestricted Software

This release of Unified Communications Manager and IM and Presence Service supports an export unrestricted (XU) version, in addition to the export restricted (K9) version.

**Note** Unrestricted versions of software are intended only for a specific set of customers who do not want various security capabilities; unrestricted versions are not intended for general deployments.

Export unrestricted versions differs from restricted versions as follows:

- Encryption of user payload (information exchange) is not supported.
- External SIP interdomain federation with Microsoft OCS/Lync or AOL is not supported.
- After you install an unrestricted release, you can never upgrade to a restricted version. A fresh install of a restricted version on a system that contains an unrestricted version is also not supported.
- All nodes within a single cluster must be in the same mode. For example, Unified Communications Manager and IM and Presence Service in the same cluster must either all be in unrestricted mode or all be in restricted mode.

- IP Phone security configurations are modified to disable signaling and media encryption (including encryption provided by the VPN phone feature).

**Note** Be aware that after you install an unrestricted release, you can never upgrade to a restricted version. You are not allowed to perform a fresh installation of a restricted version on a system that contains an unrestricted version.

For all Graphical User Interfaces (GUIs) and Command Line Interfaces (CLIs), the Administrator can view the product version (restricted or export unrestricted).

The following table describes the GUI items that are not available for the export unrestricted version ofUnified Communications Manager and IM and Presence Service.

| GUI Item | Location | Description |
|---|---|---|
| **Cisco Unified CM Administration** | | |
| **VPN Configuration** | **Advanced Features** > **VPN** | This menu and its options are not available. |
| **Phone Security Profile Configuration** | **System** > **Security** > **Phone Security Profile** | The **Device Security Mode** is set to **Non Secure** and is not configurable. |
| **Cisco Unified CM IM and Presence Administration** | | |
| **Security Settings** | **System** > **Security** > **Settings** | • You cannot check the **Enable XMPP Client to IM/P Service Secure Mode** setting.<br>• You cannot check the **Enable XMPP Router-to-Router Secure Mode** setting.<br>• You cannot check the **Enable Web Client to IM/P Service Secure Mode** setting.<br>• The option to set **SIP intra-cluster Proxy-to-Proxy Transport Protocol** to **TLS** have been removed. |
| **Service Parameter Configuration** for Cisco SIP Proxy service | **System** > **Service Parameters** and choose **Cisco SIP Proxy** as the **Service** | • All TLS options have been removed for the **Transport Preferred Order** parameter.<br>• The TLS option have been removed from the **SIP Route Header Transport Type** parameter. |

| GUI Item | Location | Description |
|---|---|---|
| **SIP Federated Domains** | **Presence** > **Inter-domain Federation** > **SIP Federation** | When you configure interdomain federation to OCS/Lync, you will receive warning popup to indicate that it is only possible to directly federate with another OCS/Lync within the enterprise. Interdomain federation to OCS/Lync outside the enterprise is not supported in unrestricted mode. |
| **XMPP Federation Settings** | **Presence** > **Inter-domain Federation** > **XMPP Federation** > **Settings** | You cannot configure the security mode. It is set to **NO TLS**. |
| **Proxy Configuration Settings** | **Presence** > **Routing** > **Settings** | You cannot set any TLS or HTTPS listeners as the preferred proxy listener. |